WHAT IS CLAIMED IS:

1. A computer-implemented method of reducing risk in a payment-based transaction wherein payment is made from an account holder to a Counterparty using a payment bank system operated by a payment bank, the method comprising the steps of:

receiving at least one user-supplied risk parameter associated with the Counterparty;

receiving a first instruction authorizing payment from the account holder to the Counterparty ;

storing the first instruction in a payment queue;

during processing of the payment transaction, performing a risk filter routine that determines whether to selectively reject payment authorized by the first instruction based upon the at least one user-supplied risk parameter associated with the Counterparty.

10007479.102201

2. The computer-implemented method of claim 1, further comprising the step of:

generating the at least one user-supplied risk parameter on a user system and communicating the at least one user-supplied risk parameter to the risk filter routine.

3. The computer-implemented method of claim 1, wherein the risk filter routine includes the steps of:

generating an available balance for the Counterparty based upon the at least one user-supplied risk parameter, payments made by the account holder, and payments received by the account holder;

reading the first instruction from the payment queue of the payment bank system; and

determining whether to selectively reject payment authorized by the first instruction based upon the available balance.

4. The computer-implemented method of claim 3, wherein payment authorized by the first instruction is rejected in the event that the amount of payment authorized by the first instruction exceeds the available balance.

5. The computer-implemented method of claim 3, wherein the first instruction is returned to the payment queue for later re-evaluation in the event that the amount of payment authorized by the first instruction exceeds the available balance.

6. The computer-implemented method of claim 3, wherein the available balance is computed over a given time period based upon payments made by the account holder in the given time period and payments received by the account holder in the given time period.

7. The computer-implemented method of claim 6, further comprising the steps of:

receiving user-supplied updates to the at least one user-supplied risk parameter; and

updating the available balance to reflect such user-supplied updates.

8. The computer-implemented method of claim 7, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.

9. The computer-implemented method of claim 6, further comprising the steps of:

receiving updates to payments made by the account holder in the given time period; and

receiving updates to payments received by the account holder in the given time period; and

updating the available balance to reflect such updates.

10. The computer-implemented method of claim 9, wherein updates to payments made by the account holder and updates to payments received by the account holder are received through data interchange with existing payments confirmation services.

11. The computer-implemented method of claim 6, further comprising the step of receiving user-supplied updates to the at least one user-supplied risk parameter for use in the risk filter routine.

12. The computer-implemented method of claim 11, further comprising the steps of: generating the user-supplied updates on a user system and communicating the user-supplied updates to the risk filter routine.

13. The computer-implemented method of claim 1, wherein the risk routine is executed by a module integrated into the payment bank system.

14. The computer-implemented method of claim 1, wherein the risk filter routine is executed by a module that communicates to the payment bank system via an application-to application interface which translates data formats between the module and the payment bank system.

15. The computer-implemented method of claim 13, wherein the at least one user-supplied risk parameter is generated on a user system and communicated to a central server, which stores the at least one user-supplied risk parameter in a data server and forwards the at least one user-supplied risk parameter to the module integrated into the payment bank system that executes the risk filter routine.

16. The computer-implemented method of claim 1, wherein the at least one user-supplied risk parameter comprises a clean payment limit.

17. The computer-implemented method of claim 1, wherein the at least one user-supplied risk parameter is associated with each payment-based transaction wherein payment is made from the account holder to the Counterparty.

18. The computer-implemented method of claim 17, wherein the at least one user-supplied risk parameter is selected from the group consisting of:

(i) currency associated with each payment-based transaction,

(ii) payment type associated with each payment-based transaction, and

(iii) a Clean Payment Limit associated with each payment-based transaction.

19. The computer-implemented method of claim 17, wherein the at least one user-supplied risk parameter is associated with a first identifier that identifies the account holder and a second identifier that identifies the Counterparty on the payment transaction.

20. The computer-implemented method of claim 1, wherein the account holder comprises a user with a pre-existing account relationship with the payment bank.

21. The computer-implemented method of claim 20, wherein the account holder further comprises a third party, and wherein the user is acting on behalf of the third party.

22. The computer-implemented method of claim 21, wherein said third party executes a third party host application that generates the at least one user-supplied risk parameter and communicates the at least one user-supplied risk parameter and associated information to a user system, which forwards the at least one user-supplied information to the risk filter routine.

23. The computer-implemented method of claim 22, wherein only the user system can forward the at least one user-supplied risk parameter communicated by the third party host application to the risk filter routine.

24. The computer-implemented method of claim 19, wherein the first and second identifiers are Bank Identifier Codes or an aggregation of such codes.

25. The computer-implemented method of claim 1, wherein the Counterparty comprises a beneficiary of the payment-based transaction.

26. The computer-implemented method of claim 25, wherein the Counterparty further comprises an intermediary to the beneficiary of the payment-based transaction.

27. The computer-implemented method of claim 1, wherein said risk filter routine cooperates with other payment processing operated by said payment bank to determine whether to selectively reject payment authorized by the first instruction.

28. The computer-implemented method of claim 1, wherein the risk filter routine cooperates with a domestic payment system operated by said payment bank, such that the first instruction is filtered by said risk filter routine for compliance with a risk profile generated from the at least one user-supplied risk parameter.

29. The computer-implemented method of claim 1, further comprising the step of : for each given first instruction, when processing by the risk filter routine rejects payment authorized by the given first instruction, adding the given first instruction to a cache of first instructions.

30. The computer-implemented method of claim 1, further comprising the step of communicating notification of rejection or success of at least one payment authorized by the first instructions stored in a cache.

31. The computer-implemented method of claim 30, wherein said notification is communicated via messaging services operably coupling the user system, a central system, and the payment bank system.

32. The computer-implemented method of claim 31, wherein a third party application is operably coupled to the payment bank system, and wherein said notification is forwarded to said third party application by said payment bank system.

33. The computer-implemented method of claim 30, wherein said notification is generated in the event that the Counterparty fails to make expected payments for a pre-determined period of elapsed time.

34. The computer-implemented method of claim 1, further comprising the steps of:

10007179 .102201

receiving a user-supplied second instruction that identifies an account holder and Counterparty; and

in response to receipt of the user-supplied second instruction, suspending all payments from the account holder to the Counterparty as identified by the second instruction.

35. The computer-implemented method of claim 34, wherein the user-supplied second instruction is generated on a user system and communicated to a central server, which stores the user-supplied second instruction in a data server and forwards the user-supplied second instruction to a module integrated into the payment bank system that executes the risk filter routine.

36. The computer-implemented method of claim 35, wherein a third party executes a third party host application that generates the user-supplied second instruction and communicates the user-supplied second instruction to a user system, which forwards the user-supplied second instruction to the module integrated into the payment bank system via the central server.

37. The computer-implemented method of claim 34, further comprising the step of: communicating notification confirming receipt and implementation of the user-supplied second instruction to the payment bank, core server, user and third party, if any.

38. The computer-implemented method of claim 1, further comprising the steps of:

receiving a third instruction that identifies a particular first instruction; and

in response to receipt of the third instruction, disabling processing of the risk filter routine for the particular first instruction.

39. The computer-implemented method of claim 38, wherein the third instruction is generated on a user system and communicated to a central server, which stores the third instruction in a data server and forwards third instruction to a module integrated into the payment bank system that executes the risk filter routine.

40. The computer-implemented method of claim 39, wherein a third party executes a third party host application that generates the third instruction and communicates the third instruction to a user system, which forwards the third instruction to the module integrated into the payment bank system via the central server.

41. The computer-implemented method of claim 39, further comprising the step of:

returning notification confirming receipt and implementation of the third instruction to the payment bank, central server, user and third party, if any.

42. The computer-implemented method of claim 39, wherein the third instruction is generated by the payment bank host application.

43. The computer-implemented method of claim 1, further comprising the steps of:

receiving a third instruction that identifies a particular Counterparty; and

in response to receipt of the third instruction, disabling processing of the risk filter routine with respect to any first instruction authorizing payment from the account holder to the Counterparty.

44. The computer-implemented method of claim 43, wherein the third instruction is generated on a user system and communicated to a central server, which stores the third instruction in a data server and forwards the third instruction to a module integrated into the payment bank system that executes the risk filter routine.

45. The computer-implemented method of claim 44, wherein a third party executes a third party host application that generates the third instruction and communicates the third instruction to a user system, which forwards the third instruction to the module integrated into the payment bank system via the central server.

46. The computer-implemented method of claim 34, further comprising the step of:

returning notification confirming receipt and implementation of the user-supplied third instruction to the payment bank, core server, user and third party, if any.

10007179.102201

47. The computer-implemented method of claim 33, wherein the third instruction is generated by the payment bank host application.

48. The computer-implemented method of claim 1, further comprising the step of: using digital certification to establish access authority and usage constraints of the risk filter routine.

49. The computer-implemented method of claim 1, wherein data transmissions are encrypted for security purposes.

50. The computer-implemented method of claim 1, wherein users and the payment bank can also generate and receive payments-related notifications, inquiries, messages and reports.

51. The computer-implemented method of claim 1, wherein users can request and receive multi-currency reports from a plurality of Payment Banks acting on their behalf.

52. The computer-implemented method of claim 1, wherein human-accessibility is provided by browser interfaces and data-accessibility is provided by electronic data interchange formats.

53. The computer-implemented method of claim 1, wherein said account holder and Counterparty comprise multiple entities that are deemed to share correlation in payment risk assessment, wherein the multiple entities are identified by an aggregate identifier.

54. The computer-implemented method of claim 1, further comprising the steps of: recording various type of information, including identification of Users, identification of Third Parties, identification of Payment Banks, identification of Counterparties, identification of Currencies, specification of the Clean Payment Limit, and Payment Type identification.

55. The computer-implemented method of claim 1, wherein selective rejection of payment authorized by the first instruction reduces payment risk arising from default by the Counterparty and any liquidity risk and system risk arising therefrom in like amount.

56. The computer-implemented method of claim 49, wherein the data transmissions occur over a virtual private network that uses the Internet and other internet protocol telecommunications networks.

57. The computer-implemented method of claim 1, wherein the risk filter routine controls the flow of payment messages from the payment queue to a domestic payment system for clearance.

58. The computer-implemented method of claim 1, wherein the first instruction comprises a S.W.I.F.T. payment transaction.

59. The computer-implemented method of claim 10, wherein updates to the payments made by the Counterparty and updates to payments received by the Counterparty comprise S.W.I.F.T. messages.

60. The computer-implemented method of claim 1, wherein the risk filter routine interoperates with a plurality of payment channels for any given currency.

61. The computer-implemented method of claim 60, wherein said plurality of payment channels includes net payment systems, real-time gross payment systems and intra-bank book transfers.

62. The computer-implemented method of claim 1, wherein the risk filter routine operates, in the event that there are multiple Counterparties of an account holder for a given first instruction, to iteratively evaluate the given first instruction for compliance with the at least one user-supplied risk parameter as applicable to each Counterparty.

63. The computer-implemented method of claim 1, wherein the Counterparty comprises one of payment beneficiary and intermediary.

64. The computer-implemented method of any of claim 34, further comprising the steps of:

receiving a user-supplied third instruction that identifies an account holder and Counterparty; and

in response to receipt of the user-supplied third instruction, reinstating payments from the account holder to the Counterparty as identified by the third instruction by countermanding a previously communicated second instruction.

10007179.102501